Math 357
Exam 02

2024–04–19 (F)

Your name: ____________________

Honor pledge:

Instructions

1. In the space above, please legibly write your name and the Rice Honor Pledge, then sign.
2. Full time for this exam is exactly 50 minutes. No resources are allowed.
3. Your reasoning—correctness and clarity—is more important than your "answer".
4. If you think there is ambiguity or error in an exercise, then briefly (!) write your understanding of the exercise and any additional hypotheses you are making, then proceed.
5. Note: The definition parts of Exercises 1–3 will be graded as Exercise 0.

This exam is an imperfect measure of my understanding at a particular point in time. It is not a measure of who I am or who I will be.

Exercise	Total	(a)	(b)	(c)	(d)
0	/4	/4	/4	/4	/4
1	/4	—	—	/4	/4
2	/4	—	/4	/4	/4
3	/4	—	/4	/4	/4
4	/4	/4	/4	/4	/4
Total	/20				

Exercise 1

Let K_0 be a field; let $n \in \mathbf{Z}_{\geqslant 0}$; and let $f = \sum_{i=0}^{n} a_i t^i = a_n t^n + \ldots + a_0 \in K_0[t]$, with $a_n \neq 0_{K_0}$. For your definitions, clearly introduce any additional objects you use and the hypotheses you make.

(a) Define what it means for f to be (i) irreducible and (ii) separable.

(b) Define the formal derivative of f. As relevant to your definition, explain what multiplication by an integer means if $\operatorname{char} K_0 \neq 0$ (in which case, K_0 does not contain an isomorphic copy of $\mathbf{Z}$).

(4 pt) For the remaining parts of this exercise, let $\operatorname{char} K_0 = 0$.

(c) Prove that if f is irreducible, then f is separable.

(d) Give a counterexample that illustrates that the converse to the statement in part (c) is false. That is, give a polynomial f that is separable and reducible.

Solution: Part (a): (i) By hypothesis, K_0 is a field, hence an integral domain. Thus $K_0[t]$ is an integral domain, so the general definition of an irreducible element of an integral domain applies. Specifically, let $f \in K_0[t]$ such that $f \neq 0$ (the zero polynomial) and $f \notin (K_0[t])^\times \cong K_0^\times$.[1] Then f is **irreducible** if for all $f_1, f_2 \in K_0[t]$ such that $f = f_1 f_2$, either $f_1 \in (K_0[t])^\times$ or $f_2 \in (K_0[t])^\times$.[2]

(ii) A polynomial $f \in K_0[t]$ is **separable** if f each zero of f (for example, in some splitting field for f) has multiplicity one.

Note that the definition of irreducible depends on the ring of coefficients (for example, $f = 2t$ is irreducible in $\mathbf{Q}[t]$ and reducible in $\mathbf{Z}[t]$), whereas the definition of separable does not (if each zero of f has multiplicity one for some splitting field for f, then the same is true for any splitting field for f, because any two splitting fields for f are isomorphic).

Part (b): Given

$$f = \sum_{i=0}^{n} a_i t^i = a_n t^n + a_{n-1} t^{n-1} + \ldots + a_1 t + a_0$$

the formal derivative of f is the polynomial[3]

$$D_t f = \sum_{i=1}^{n} i \cdot a_i t^{n-1} = n \cdot a_n t^{n-1} + (n-1) \cdot a_{n-1} t^{n-2} + \ldots + a_1$$

In general, given a positive integer m and a ring element r, the notation $m \cdot r$ (often written without the dot) denotes the sum of m copies of the element r:

$$m \cdot r = \sum_{i=1}^{m} r$$

[1] The units in $K_0[t]$ are the constant polynomials whose constant value is a unit in K_0. Because K_0 is a field, by definition every nonzero element of K_0 is a unit.

[2] See DF3e, p 284.

[3] See DF3e, p 546.

By the distributive axiom for a field, this is equivalent to

$$m \cdot r = \left(\sum_{i=1}^{m} 1_{K_0} \right) r$$

Part (c): For an arbitrary field K_0, we have seen that a polynomial $f \in K_0[t]$ is separable if and only if $\gcd(f, D_t f) = 1$. Let $f \in K_0[t]$ be irreducible, and denote $n = \deg f$. The definition of irreducible and the hypothesis that K_0 is a field imply that f cannot be a constant function, so $n \geqslant 1$. By hypothesis, $\operatorname{char} K_0 = 0$, so $D_t f = n - 1$. Also by hypothesis, f is irreducible, so by definition if $f = f_1 f_2$, then one of the f_i, say f_1, is a unit, which in turn implies that $\deg f_1 = 0$ and $\deg f_2 = \deg f - \deg f_1 = \deg f$. Because $\deg D_t f = n - 1 < n = \deg f$, it follows that $D_t f$ is a factor of f if and only if $\deg D_t f = 0$. This implies that $\gcd(f, D_t f) = 1$, which is equivalent to f being separable.

Part (d): A field is an integral domain. By definition, an integral domain has at least two distinct elements, 0 and 1 (the additive identity and the multiplicative identity, respectively, in the ring). Hence for any field K_0, the polynomial $f = (t-0)(t-1) = t^2 - t$ is separable and reducible, by construction.

Exercise 2

For your definitions, clearly introduce the objects you use and the hypotheses you make.

(a) Define "minimal polynomial".

(4 pt) For the remaining parts of this exercise, let $\alpha = \sqrt[3]{5 - 3\sqrt{-1}} \in \mathbf{C}$.

(b) Find the minimal polynomial $m_{\alpha,\mathbf{Q}}$ of α over $\mathbf{Q}$. Demonstrate that it satisfies the axioms (i.e. defining properties) in your definition in part (a).

(c) Prove that $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 6$.

(d) Let $f \in \mathbf{Q}[t]$ such that $\deg f = 4$ and f has no zeros in $\mathbf{Q}$, and let $\beta \in \mathbf{C}$ satisfy $f(\beta) = 0$. Can $\beta \in \mathbf{Q}(\alpha)$? Justify.

Solution: Part (a): Let $K : K_0$ be a field extension, and let $\theta \in K$ be algebraic over K_0. The **minimal polynomial of** θ **over** K_0, denoted m_{θ,K_0}, is the unique monic, irreducible polynomial for which θ is a zero.[4]

In this definition, irreducible is equivalent to minimal degree, in the following sense: Let $m \in K_0[t]$ such that $m(\theta) = 0$. Then m is irreducible if and only if m is a nonzero polynomial with minimal degree among the nonzero polynomials that have θ as a zero.

Part (b): We compute

$$\begin{aligned} \alpha = \sqrt[3]{5 - 3\sqrt{-1}} \quad &\Leftrightarrow \quad \alpha^3 = 5 - 3\sqrt{-1} \quad \Leftrightarrow \quad \alpha^3 - 5 = -3\sqrt{-1} \\ &\Rightarrow \quad (\alpha^3 - 5)^2 = 9(-1) \quad \Leftrightarrow \quad \alpha^6 - 10\alpha^3 + 34 = 0 \end{aligned}$$

Viewing this last expression as a polynomial function evaluated at $t = \alpha$, we define

$$m = t^6 - 10t^3 + 34 \in \mathbf{Q}[t]$$

This polynomial is in $\mathbf{Q}[t]$ and is monic (by inspection), is irreducible (for example, by the Eisenstein–Schönemann criterion with the prime 2), and has α as a zero (by construction). Thus by definition, it is the minimal polynomial of α over $\mathbf{Q}$.

Part (c): In the setting of our definition in part (a), we have shown that

$$[K_0(\theta) : K_0] = \deg m_{\theta,K_0}$$

Applying this to part (b) gives the desired result.

Part (d): Yes, it is possible for $\beta \in \mathbf{Q}(\alpha)$. The hypotheses that $f \in \mathbf{Q}[t]$ and $f(\beta) = 0$ implies that $m_{\beta,\mathbf{Q}} \mid f$. By hypothesis, f has no zeros in $\mathbf{Q}$, which is equivalent to the statement that a factorization of f into irreducible elements in $\mathbf{Q}[t]$ has no factors of degree 1; however, it may have factors of degree 2. If $\deg m_{\beta,\mathbf{Q}} = 2$, then $\beta \in \mathbf{Q}(\alpha)$ is not precluded by the tower law. More precisely, if $\beta \in \mathbf{Q}(\alpha)$, then $\mathbf{Q}(\beta) \subseteq \mathbf{Q}(\alpha)$. Viewing both fields as extensions of the base field $\mathbf{Q}$, we get the tower $Q(\alpha) : \mathbf{Q}(\beta) : \mathbf{Q}$, so the tower law gives

$$[\mathbf{Q}(\alpha) : \mathbf{Q}] = [\mathbf{Q}(\alpha) : \mathbf{Q}(\beta)][\mathbf{Q}(\beta) : \mathbf{Q}]$$

[4] See DF3e p 520.

In particular, this implies that

$$\deg m_{\beta,\mathbf{Q}} = [\mathbf{Q}(\beta) : \mathbf{Q}] \text{ divides } [\mathbf{Q}(\alpha) : \mathbf{Q}] = 6$$

Let's give a concrete example of such an $f \in \mathbf{Q}[t]$ and $\beta \in \mathbf{C}$. Let

$$f = t^4 - t^2 - 2 = (t^2 + 1)(t^2 - 2) \qquad\qquad \beta = \sqrt{-1} \in \mathbf{C}$$

It is straightforward to check that $\deg f = 4$, f has no zeros in $\mathbf{Q}$, and $f(\beta) = 0$. Moreover, from the definition of α, we get

$$\beta = \sqrt{-1} = -\frac{1}{3}(\alpha^3 - 5)$$

so $\beta \in \mathbf{Q}(\alpha)$, as desired.

Exercise 3

For your definitions, clearly introduce the objects you use and the hypotheses you make.

(a) Define "splitting field".

(4 pt) Let $p, q \in \mathbf{Z}_{>0}$ be prime; let

$$f = t^p - q \qquad\qquad g = \sum_{j=0}^{p-1} t^j = t^{p-1} + \ldots + t + 1$$

be polynomials in $\mathbf{Q}[t]$; fix a splitting field K for fg, the product of f and g, over $\mathbf{Q}$; let $\alpha \in K$ be a zero of f; let $\zeta \in K$ be a zero of g; and let K_f (respectively, K_g) be the splitting field for f (respectively, g) in $K : \mathbf{Q}$.

(b) Prove that f and g are irreducible in $\mathbf{Q}[t]$. *Hint:* For g, let $\tilde{g}(t) = (t-1)g(t) = t^p - 1$, and consider $\tilde{g}(t+1)$.

(c) Prove that for each integer $k \in \{0, \ldots, p-1\}$, ζ^k is a zero of $\tilde{g}$, and $\zeta^k\alpha$ is a zero of f. Deduce that $K = K_f K_g$, the composite field of K_f and K_g in K.

(d) Prove that $[K : \mathbf{Q}] = p^2 - p$. *Hint:* Use a field diagram.

Solution: Part (a): Let $K : K_0$ be a field extension, and let $f \in K_0[t]$. K is a **splitting field for** f (over K_0) if (i) f splits completely (that is, factors as a product of linear factors) in $K[t]$; and (ii) for all proper intermediate fields in $K : K_0$ (that is, all fields K_i such that $K_0 \subseteq K_i \subset K$), f does not split completely in $K_i[t]$.[5] We have seen that for all fields K_0 and for all polynomials $f \in K_0[t]$, there exists a splitting field for f, and that it is unique up to isomorphism.

Part (b): f is irreducible by the Eisenstein–Schönemann criterion with the prime q. For g, note that

$$\begin{aligned} tg(t+1) = \tilde{g}(t+1) = (t+1)^p - 1 &= t^p + \binom{p}{p-1} t^{p-1} + \ldots + \binom{p}{1} t + 1 - 1 \\ &= t\left(t^{p-1} + \binom{p}{p-1} t^{p-2} + \ldots + \binom{p}{1}\right) \end{aligned}$$

Because $K_0[t]$ is an integral domain,[6] we may cancel t from both sides of this equation to get

$$g(t+1) = t^{p-1} + \binom{p}{p-1} t^{p-2} + \ldots + \binom{p}{1}$$

Because p is prime, for all $i \in \{1, \ldots, p-1\}$,

$$p \mid \binom{p}{i} = \frac{p!}{i!(p-i)!}$$

which are precisely the nonleading coefficients of $g(t+1)$. Moreover, $p \nmid 1 = \mathrm{LC}(g(t+1))$; and $p^2 \nmid p = \binom{p}{1}$, the constant term of $g(t+1)$. Thus by the Eisenstein–Schönemann criterion with

[5] See DF3e p 536.

[6] As we noted in our response to Exercise 1(a), K_0 is a field implies K_0 is an integral domain implies $K_0[t]$ is an integral domain.

prime p, $g(t+1)$ is irreducible in $\mathbf{Z}[t]$, hence $g(t)$ is irreducible in $\mathbf{Z}[t]$. Hence by Gauß's lemma, g is irreducible in $\mathbf{Q}[t]$.

Part (c): By hypothesis, ζ is a zero of g, so

$$\zeta^p - 1 = \tilde{g}(\zeta) = (\zeta - 1)g(\zeta) = 0 \qquad \Leftrightarrow \qquad \zeta^p = 1$$

Let $k \in \{0, \dots, p-1\}$. We compute

$$\tilde{g}(\zeta^k) = (\zeta^k)^p - 1 = (\zeta^p)^k - 1 = 1^k - 1 = 0$$

Similarly,

$$f(\zeta^k \alpha) = (\zeta^k \alpha)^p - q = (\zeta^p)^k \alpha^p - q = \alpha^p - q = f(\alpha) = 0$$

For $k \in \{0, \dots, p-1\}$, $\zeta^k = 1$ if and only if $k = 0$.Thus the values $1, \zeta, \dots, \zeta^{p-1}$ are distinct, so $\zeta, \dots, \zeta^{p-1}$ are the $p - 1 = \deg g$ zeros of g, and $\alpha, \zeta\alpha, \dots, \zeta^{p-1}\alpha$ are the $p = \deg f$ zeros of f. By definition, a splitting field K_f for f contains all zeros of f, so in particular $\alpha, \zeta\alpha \in K_f$. Because fields are closed under the field operations (addition, multiplication, and taking inverses), it follows that

$$\zeta = \alpha^{-1} \cdot \zeta\alpha \in K_f$$

so for all $k \in \mathbf{Z}$, $\zeta^k \in K_f$. Therefore

$$K = \mathbf{Q}(\zeta, \alpha) = K_f$$

Part (d): Consider a field diagram with the fields $K = \mathbf{Q}(\zeta, \alpha) = K_f K_g$, $\mathbf{Q}(\zeta), \mathbf{Q}(\alpha)$, and $\mathbf{Q}$. Note that

$$K = K_f K_g = \mathbf{Q}(\zeta, \alpha)\mathbf{Q}(\zeta) = \mathbf{Q}(\zeta, \alpha)$$

Because

$$\begin{aligned} [\mathbf{Q}(\zeta) : \mathbf{Q}] &= \deg m_{\zeta,\mathbf{Q}} = \deg g = p - 1 \\ [\mathbf{Q}(\alpha) : \mathbf{Q}] &= \deg m_{\alpha,\mathbf{Q}} = \deg f = p \end{aligned}$$

and $\gcd(p, p-1) = 1$, the tower law implies that

$$[K : \mathbf{Q}] = p(p-1) = p^2 - p$$

Exercise 4

(4 pt) Let $K : K_0$ be a field extension.

(a) Define $\mathrm{Aut}(K : K_0)$.

(b) Let H be a subgroup of $\mathrm{Aut}(K : K_0)$. Define the fixed field of H.

(c) State what it means for $K : K_0$ to be galois. You may use any characterization of a galois extension that we have discussed in class.

(d) When $K : K_0$ is galois, the fundamental theorem of galois theory gives an inclusion-reversing, bijective correspondence between subfields (intermediate fields) of $K : K_0$ and subgroups of the galois group $\mathrm{Gal}(K : K_0)$. Define the map from subfields to subgroups, and the map from subgroups to subfields.

Solution: Part (a): The **automorphism group** of the field extension $K : K_0$ is the set of automorphisms of K (that is, field isomorphisms from K to itself) that fix the base field K_0 (pointwise):[7]

$$\mathrm{Aut}(K : K_0) = \{\sigma : K \to K \mid \sigma \text{ is an isomorphism}; \forall a \in K_0, \sigma(a) = a\}$$

equipped with the group operation of function composition.

Part (b): The **fixed field** of H, denote it $\mathcal{F}(H)$, is the set of elements of the extension field K that are fixed by all automorphisms in H:[8]

$$\mathcal{F}(H) = \{\alpha \in K \mid \forall \sigma \in H, \sigma(\alpha) = \alpha\}$$

Part (c): The definition of a galois extension that we gave in our development of galois theory was that a finite extension $K : K_0$ is **galois** if $\mathrm{Aut}(K : K_0) = [K : K_0]$. Equivalent characterizations include[9]

(1) There exists a separable $f \in K_0[t]$ such that K is a splitting field for f.

(2) $\mathcal{F}(\mathrm{Aut}(K : K_0)) = K_0$.

(3) $K : K_0$ is finite, normal, and separable.

Part (d): The maps are

$$\begin{aligned} \{\text{subfields } K_i \text{ in } K : K_i : K_0\} &\leftrightarrow \{\text{subgroups } H \leqslant \mathrm{Gal}(K : K_0)\} \\ K_i &\mapsto \mathrm{Aut}(K : K_i) \\ \mathcal{F}(H) &\leftarrow\!\shortmid H \end{aligned}$$

Note that these maps are inverse to each other.

[7] See DF3e, p 558.
[8] See DF3e, p 560.
[9] See DF3e, pp 562 and 574.